IN THE SPECIFICATION:

Please replace the first paragraph of the "SUMMARY OF INVENTION" with the following paragraph:

The present invention relates generally to an integrated optics encryption device. The preferred embodiment of the invention is an integrated optics encryption device comprising a coherent light source connected to a multi-function integrated optics chip (MIOC). The MIOC comprises two divergent paths with mirrored ends. The MIOC also has an encrypted message output. One path is connected to a message signal input that can alter the refractive index of the path. The other path is connected to a key signal input that can alter the refractive index of the other path. The two paths form portions of two legs of an interferometer whose intensity output is proportional to the total phase difference between light waves traveling in the two paths.

Please replace the section titled "DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS" as follows:

---

(1) The following description is provided to enable any person skilled in the art to make and use the invention and sets forth the best modes contemplated by the inventors of carrying out his invention. Various modifications, however, will remain readily apparent to those skilled in the art, since the general principles of the present invention have been defined herein specifically to provide an integrated optics encryption device.

(2) Referring now to Figure 1, a preferred embodiment of an integrated optics encryption device 10 comprises a coherent light source 20. In the preferred embodiment, the coherent light source 20 is a laser, including but not limited to a laser diode. The coherent light source 20 is connected by fiber optic link 25 to a

multi-function integrated optics chip (MIOC) 30. The MIOC 30 in the preferred embodiment comprises a lithium-niobate chip. In the embodiment of Figure 1, the MIOC 30 comprises two divergent paths 40 and 50 with ends 45 and a loop 60. The MIOC also has an encrypted message output 70.

(3) Referring to Figure 4, the MIOC 30 in an alternative embodiment comprises two divergent paths 40 and 50 with ends 45, each end 45 being mirrored to reflect light signals. In a preferred embodiment, each end 45 is coated with a metallic film or a multi-layer dielectric film to form a reflector for each path 40 and 50. Referring to Figure 5, the MIOC 30 in another alternative embodiment comprises two divergent paths 40 and 50 meeting at a convergent end 47 connected to the encrypted message output 70.

(4) In each embodiment, one path 40 is controlled by a message signal input 80 that can reversibly alter the refractive index of the path 40. The message signal input 80 is preferably a pair of metal electrodes attached to the MIOC 30 that receive signals that change the voltage between the electrodes and alter the refractive index of the path 40 on the MIOC 30. By altering the refractive index of the path 40, the message signal input 80 can allow a light signal to combine coherently with a light signal passing through path 50, to produce a maximum or minimum intensity output 57 when they recombine at junction 55. The message signal input 80 is typically connected to message signal generating means such as a pulse signal generator, computer or any other source of digital signal input.

(5) In each embodiment, one path 50 is controlled by a key signal input 90 that can reversibly alter the refractive index of the path 50. The key signal input 90 is preferably a pair of metal electrodes fabricated on the MIOC 30 that receive signals that change the voltage between the pads and alters the refractive index of the MIOC 30, within the path 50. By altering the refractive index of the path 50, the key signal input 90 can allow a light signal to combine coherently with a light signal through path 50 to produce a maximum or minimum intensity output

when they recombine at junction 55. The key signal input 90 is typically connected to a key signal generating means such as a pulse signal generator, computer or any other source of digital signal input. It can also be connected to another MIOC. It is preferred that the key signal generating means act as a random number generator.

(6) One embodiment of the encryption process is shown in Figure 2. Upper signal level 86 indicated in Figure 2 corresponds to a $\Pi/2$ radian phase shift for the message signal 85. Lower signal level 87 of message signal 85 is a 0-radian phase shift. Lower signal level 97 of key signal 95 corresponds to a Π radian phase shift whereas upper signal level 96 of key signal 95 corresponds to a $3\Pi/2$ phase shift. Preferably, the key signal 95 is from a random number generator. It should be noted that the voltage levels applied to the electrodes 80 and 90 on the MIOC 30, and hence, the relative phase shift between the optical wave, only exist for a time T (tau) equal to the time required for each optical wave to propagate from one signal input, through the interferometer/MIOC 30, to the other signal input. Therefore, the voltage levels applied to the electrodes must be charged every T (tau). The message signal 85 and the key signal 95 are kept in phase by a software driver program.

(7) To summarize, a coherent light signal is split between two paths 40 and 50. If neither a message signal 85 nor a key signal 95 is input, the divided light signal cancels itself out and no encrypted message signal 100 is emitted. When either a message signal 85 or a key signal 95 are input alone, the MIOC 30 emits an encrypted message signal 100 from the encrypted message output 70. When both a message signal 85 and a key signal 95 are input the light signals cancel each other out and no encrypted message signal 100 is emitted. In Figure 2, the message signal 85 is transformed by the key signal 95 to the encrypted message signal 100. This is an "Exclusive Or" (XOR) encryption algorithm and a symmetric encryption algorithm.

(8) Thus, the simple encryption table in Figure 3 becomes apparent. In the 0,0 position of Figure 3, neither a message signal 85 nor a key signal 95 are input. Thus, no encrypted message signal 100 results. In the 0,1 position of the table, no message signal 85 is input and a key signal 95 is input. Thus, an encrypted message signal 100 results. Again, an "Exclusive Or" algorithm is depicted.

(9) A method for encryption using interference from a coherent light source therefore becomes apparent. The method comprises the following steps:

(10) Issuing a coherent light signal from a coherent light source 20 through a fiber optic link 25 to a multi-functional integrated optics chip 30;

(11) Dividing the coherent light signal along two paths 40 and 50 within the multi-functional integrated optics chip 30;

(12) Issuing pre-determined signals 85 and 95, respectively, from a message signal input 80 attached to one path 40 of the multi-functional integrated optics chip 30 and a key signal input 90 attached to the other path 50;

(13) Recombining the divided light signal to create an encrypted message signal 100; and,

(14) Issuing the encrypted signal from an encrypted message output 70.

(15) Another user with an identical key signal 95 can decrypt the encrypted message signal 100 by using the above method and substituting the encrypted message signal 100 for the message signal 85. The resulting signal issued by the device will be the original message signal 85. By applying the key signal 95 to the encrypted message signal 100, the message signal 85 appears and can be read by a photodiode as any other digital signal or message clear text detailed in the prior art.

(16) Therefore, the present invention has several advantages over the prior art. The preferred embodiments of the invention and the method of using them rapidly encrypt a message signal 85 as it is generated by simultaneously

applying a key signal 95 using hardware instead of software. Translation from message signals to encrypted signals occurs rapidly in comparison to software data encryption methods. The preferred embodiment of the invention can operate at 10 gigahertz (10GHz) or higher. A user may still utilize prior art software encryption methods in addition to the present invention for increased security. The "Exclusive Or" algorithm detailed herein also doesn't require the use of public keys and/or prime numbers. In fact, when the key signal 95 comes from a random number generator, this invention creates a stream cipher that approximates a "one-time pad." A "one-time pad" is generally assumed to be an unbreakable method of encryption when a potential eavesdropper has no access to the one-time pad.

a2

(17) In each of the above embodiments, the different positions and structures of the present invention are described separately in each of the embodiments. However, it is the full intention of the inventor of the present invention that the separate aspects of each embodiment described herein may be combined with the other embodiments described herein. Those skilled in the art will appreciate that adaptations and modifications of the just-described preferred embodiment can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

IN THE DRAWINGS:

Please replace Figures 1, 2 and 3 with the revised Figures 1, 2 and 3 enclosed.

No new matter has been added.